**IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA**
**Richmond Division**

| | |
|---|---|
| COURTHOUSE NEWS SERVICE,<br><br>Plaintiff,<br><br>v.<br><br>JACQUELINE C. SMITH, in her official capacity as Clerk of the Circuit Court for Prince William County, Virginia,<br><br>Defendant,<br><br>and<br><br>THE COMMONWEALTH OF VIRGINIA,<br><br>Intervenor-Defendant. | Civil Action No. 3:21-cv-00460-HEH |

**DEFENDANT COMMONWEALTH OF VIRGINIA'S BRIEF IN OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT**

The Commonwealth of Virginia (the "Commonwealth"), by counsel, hereby responds to Plaintiff Courthouse News Service's ("CNS") Motion for Summary Judgment. CNS has failed to articulate a restriction to its rights under the First Amendment. But even if the Court determines that requiring the public to view court records at the courthouse is a First Amendment restriction, that restriction is subject to relaxed scrutiny. CNS has likewise failed to show that it is entitled to OCRA access under the Code of Virginia. Finally, CNS has failed to show that the Commonwealth would effectively achieve its interest in the fair and orderly administration of justice absent the non-attorney access and dissemination restrictions because redaction, subscriber agreements, and sealing are ineffective at preventing harmful data harvesting.

**LISTING OF DISPUTED FACTS**
**PURSUANT TO LOCAL CIVIL RULE 56**

1. The Commonwealth disputes the facts contained in Dkt. No. 71 ¶ 9. While the Commonwealth stipulated to the facts included in Dkt. No. 55 ¶ 10, the Commonwealth disputes the allegations contained in Dkt. No. 71-1, which are incorporated into paragraph 9 of CNS's listing of undisputed facts. Specifically, the Commonwealth disputes that "[t]he overwhelming number of states and courts that have engaged in the technological transition have given access to their records online . . . through a court website." *Id.* ¶ 26. The degree to which some states, and individual courts within states, have made all nonconfidential court records available online to the general public, is a disputed fact.

The Commonwealth additionally avers that the information contained in Dkt. No. 71 ¶ 8 is irrelevant. The record is devoid of any facts as to those states' policy interests in protecting the privacy of their litigants; the record is likewise devoid of any facts showing that those systems of remote access effectively achieve those interests. In contrast, Virginia has articulated an interest in protecting the privacy of its litigants, and in protecting personal privacy generally. Va. Code § 17.1-293(A)-(B); Va. Code § 59.1-442 (the "Personal Information Privacy Act"). This Court is tasked only with deciding whether the Commonwealth would achieve these interests less effectively absent the non-attorney access and dissemination restrictions. *Ross v. Early*, 746 F.3d 546, 552 (4th Cir. 2014). Other states' practices with regards to remote access to court records have no bearing on this analysis without further facts as to their interests in protecting personal privacy and how their systems achieve those interests.

In the event of a trial, the Commonwealth would demand proof of the online access practices described in the states listed in both Dkt. Nos. 71 ¶ 9 and 71-1 ¶ 27, and for the states where individual courts provide such access, evidence of those practices by each court.

2. The Commonwealth disputes that handwritten notes present on a draft of the 2018 Work Group Report, Dkt. No. 71-14, "reflect its view that no authority may exist for clerks' concerns that non-attorney OCRA users could scrape data." Dkt. No. 71 at 10 ¶ 33.The Work Group Report stated that "[i]f the [statewide e-filing] system is publicly available, there is a high probability that certain entities will scrape the data and make the information available in commercial databases that are not under the control of OES." Dkt. No. 71-14 at 5. Alisa Padden, then Staff Attorney for OES, in response to this statement, commented: "What's the authority for this? Has it happened in other states?" *Id.*; *see also* Dkt. No. 71-13 (listing Alisa Padden as one of seven OES employees and nineteen individuals total, who "participated in the development of [the 2018 Work Group] report."). This handwritten question, added to a working draft of the report by a single individual in 2018, does not represent OES's "view that no authority may exist for clerks' concerns that non-attorney OCRA users could scrape data" in 2022. Dkt. No. 71 at 10 ¶ 33. As has been developed on the record, OES has confirmed that every publicly accessible system that it has developed has been subject to data harvesting. Dkt. No. 67 at 5-9 (discussing how General OCIS, Circuit OCIS, OCIS 2.0, and the VDBC have been mined by bots for information, with the VDBC in particular being mined for social security numbers). The Commonwealth additionally maintains that this Court can take judicial notice that data brokers routinely mine court records for information on litigants, often to target the financially vulnerable. Office of Oversight and Investigations Majority Staff, A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, Dec. 18, 2013, https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577 at "Executive Summary" (hereinafter, the "Data Broker Report"); Fred H. Cate, *Government Data*

*Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 457 (2008).

3. The Commonwealth disputes that the privacy measures described in Dkt. No. 71 ¶¶ 43-44 achieve the Commonwealth's interest in protecting the privacy interests of its litigants. Specifically, CNS states that "[m]any circuit court cases that concern minors are confidential by statute and thus not available on OCRA", "[m]aiden names are . . . often sealed from public view", and "minor names may be sealed where the health, safety or liberty of the child is in jeopardy", and *Id.* (citations omitted). Sealing the information described in these paragraphs does not address the wide array of private information contained in state court records. *See infra* at 21. And by the qualified language it uses ("many," "often" and "may be"), CNS admits that Virginia courts can only seal or protect this particular information on a case-by-case basis.

## ARGUMENT

### I. The Constitution does not require Virginia clerks to provide unlimited remote public access to court records, but if the Court finds that requiring the public to visit a courthouse limits CNS's First Amendment rights, that limitation is nevertheless subject to relaxed scrutiny.

There is no First Amendment right to remote access to court records. No court has found that requiring records requesters to visit the courthouse to obtain copies of records violates the First Amendment, nor has CNS argued that the public has a fundamental right to remotely access civil court records. *See* Memo. Op. at 9, Dkt. No. 48. This otherwise constitutional requirement is not rendered violative of the First Amendment if a clerk chooses to offer remote record access to officers of the court. *Cf.* Dkt. No. 1 ¶ 41 ("While a Virginia Circuit Court clerk need not make its documents available for remote or online viewing, once a clerk does so . . . it becomes incumbent on the clerk to offer that same access to all members of the public and the press."). But should the Court be inclined to view courthouse visitation as restrictive to CNS's First Amendment rights, the Court should examine the non-attorney access and dissemination

restrictions under relaxed scrutiny.

A. There is no First Amendment right to remote access to court records.

No court has held that the First Amendment requires more access to court records than can be granted at the courthouse. The Supreme Court has explicitly held only that there is a First Amendment right of public access to criminal trials and criminal trial-like proceedings, and has never addressed the question of whether there is a constitutional right of access to civil proceedings or to court records. David S. Ardia, *Court Transparency and the First Amendment*, 38 Cardozo L. Rev. 836, 840 (2017). In the Fourth Circuit, only in 2021 was the First Amendment right of access to the courts extended to include access to civil complaints. *Courthouse News Serv. v. Schaefer*, 2 F.4th 318, 326 (4th Cir. 2021) ("*Schaefer*"). In *Schaefer*, the Fourth Circuit applied the "experience and logic test" to conclude that the "First Amendment right of access exists as to *some* documents submitted in conjunction with judicial proceedings that themselves would trigger a right of access," but that the public also has a right of access to nonconfidential civil complaints and docket sheets independently from the right to observe a judicial proceeding. *Id.* at 326-27 (internal quotations omitted) (emphasis added).

But the right of access the Fourth Circuit found in *Schaefer* is not unlimited. "This flexible standard does not require perfect or instantaneous access" because "the Constitution does not require the impossible." *Id.* at 328. "Rather, it provides courts with some leeway where same-day access would be impracticable, and fully exempts inconsequential delays and those caused by extraordinary circumstances." *Id.* Delays in accessing civil complaints must be "content-neutral, narrowly tailored and necessary to preserve the court's important interest in the fair and orderly administration of justice." *Id.* Accordingly, the court held that the defendant clerks had arbitrarily delayed the public's access to civil complaints, finding that the clerks could

end delays of public access to civil complaints "without changing any policies, hiring any new employees, or increasing employees' hours." *Id.* at 329. Although the clerks attempted to show "possible explanations" for the delays that occurred prior to the lawsuit, "they failed to offer facts establishing that any of these explanations action did actually cause delays." *Id.* The court observed that if the clerks "had conclusively demonstrated that the delays during this period were . . . due to inclement weather or a security threat, for example – the result might well be different." *Id.* Without that factual justification, however, the court held that the delays in accessing newly filed complaints were arbitrary and therefore an unconstitutional infringement on the public's right to access court records. *Id.*

In this case, however, any "delay" caused by OCRA's non-attorney access limitation is, in fact, due to cyber security threat. In contrast to the factually empty justifications offered by the clerks in *Schaefer*, cyber security threats to digital records compiled by the government are well-known matters of public record recognized by both Congress and the Supreme Court of the United States. *See* Dkt. No. 67 at 4-5 (discussing the Data Broker Report); *see also infra* at 7-9, 14-23. Furthermore, the Defendants have put forth uncontested evidence that granting the general public OCRA access would require a change in policies, hiring new employees or increasing the hours worked by existing employees, and expenditure of funds to build the server infrastructure for the increased traffic. *See, e.g.*, Dkt. No. 69-1, ¶¶ 6, 10-11 (Declaration of Arlington County Clerk as to costs and labor expended to comply with redaction requirements for public access to online court records); Dkt. No. 67-1 (Declaration of IT Manager for the Commonwealth detailing ongoing efforts by state employees to combat data mining on publicly-accessible court records databases). To paraphrase the Fourth Circuit: with this evidence, the result in this case should well be different than the result reached in *Schaefer*. *Id.* at 329.

The cyber security threat that justifies the non-attorney access limitation additionally illustrates why no court has found a right to remotely access data compiled by the government. As the Supreme Court has noted, mass data dissemination intrudes on privacy interests, even when that same information is disseminated in other circumstances. *See generally U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749 (1989) ("*Reporters Committee*"); *see also U.S. Dep't of Def. v. Fed. Labor Relations Auth.*, 510 U.S. 487, 500 (1994) ("An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.")

In *Reporters Committee*, reporters ("respondents") sought, under the Freedom of Information Act ("FOIA"), criminal "rap sheets" compiled by the Department of Justice and the Federal Bureau of Investigation on a group of people alleged to be "organized crime figures" accused of bribing a Congressman. *Id.* at 757. Rap sheets "contain certain descriptive information, such as date of birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations of the subject." *Id.* at 752. "Because events summarized in a rap sheet have been previously disclosed to the public," the respondents contended that the subject of the rap sheet had no privacy interest in the disclosure of the compiled information. *Id.* at 762-63.

The Supreme Court "reject[ed] respondents' cramped notion of personal privacy." *Id.*

> [T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly, there is a vast difference between the public records that might be found after a diligent search of courthouse files . . . throughout the country and a computerized summary located in a single clearinghouse of information.

*Id.* at 764. The Supreme Court found that the compilation of data *heightened* the individual's privacy interest in the amassed information: "The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation . . . the privacy interest . . . is in fact at its apex . . ." *Id.* at 780; *see also Whalen v. Roe*, 429 U.S. 589, 607 (1977) (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information . . .").

While the Court in *Reporters Committee* analyzed these considerations within the prism of FOIA disclosure, the Court's holding is instructive as to why a right to mass data compiled by the government is nonexistent under the First Amendment or otherwise. There is no right to unlimited remote access to "cumulative, indexed, computerized data," *id.* at 760, because such a right would, in turn, infringe upon individuals' privacy interests, which are heightened when the government compiles personal information into a single place.

In *Reporter's Committee*, the information in the rap sheet was relatively non-sensitive and limited in scope, such as charges, convictions, incarcerations. 489 U.S. at 752. In contrast, state court records contain a far broader assortment of sensitive information, including data relating to individuals' location, identity, health, assets, financial information, employment, sexual activities, and education. David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 Berkeley Tech L.J. 1807, 1860 at Table 4 (hereinafter, the 2015 Empirical Study). Sensitive information appears in state court records at an extremely high rate, even when redaction laws are put in place. *See id.* at 1881-1891.[1] And in Virginia, there is no

[1] For further discussion, *see* Dkt. No. 67 at 21-23; *see also infra* at 18-21.

way to segregate a user's access to particular records in OCRA. Dkt. No. 67-2, ¶ 7. Once a user has access, they have access to every record uploaded to OCRA, both civil and criminal. *Id.* This compilation heightens the privacy risk for the individuals described in the records, because as noted *supra*, court records are routinely mined for personal information, which is then sold at the expense of the most vulnerable litigants;[2] if there were a First Amendment right to remotely access compiled data, such as court records, there is no reason to believe that Virginia's court records would not be mined and exploited in the same fashion. On the contrary, Defense witness Joby Knuth is prepared to testify as to the ongoing "bot" attacks on state records databases to scrape information. Dkt. No. 67-1, ¶¶ 9-16. Finding a First Amendment right to remotely access court records would leave the Commonwealth "transformed in one fell swoop into *the* clearinghouse for highly personal information, releasing records on any person, to any requester, for any purpose." *Reporters Comm.* 489 U.S. at 761 (emphasis in the original) (quotation omitted). The First Amendment does not require Virginia to facilitate this exploitation of its own litigants.

B. If the Court is inclined to view OCRA's non-attorney access and dissemination limitations as restrictive to CNS's First Amendment rights, the Court should apply relaxed scrutiny because they resemble "time, place, and manner" restrictions.

Although CNS does not dispute that the challenged restrictions are content-neutral and viewpoint neutral, CNS argues that requiring the public to visit the courthouse during business hours to gain access to court records is a "total restraint on the public's first amendment right of access . . ." and therefore, strict scrutiny applies, directly disputing this Court's analysis in deciding the motions to dismiss. Dkt. No. 71 at 20 (quoting *Associated Press v. Dist. Ct.*, 705

[2] Office of Oversight and Investigations Majority Staff, A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, Dec. 18, 2013, https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577 at "Executive Summary."

F.2d 1143, 1147, 1149 (9th Cir. 1983)); *cf.* Memo. Op. at 10, Dkt. No. 48.

But not only is *Associated Press* not binding on this Court, the Ninth Circuit Court of Appeals was silent as to levels of scrutiny and involved a blanket restriction on access to documents. In that case, appellants challenged a district judge's order sealing every single document filed in a certain case. *Id.* at 1144. Specifically, the judge, in response to wide press coverage, ordered that "all future filings of documents" in the matter would need to be filed *in camera* and under seal. *Id.* The order "was not accompanied by any findings" and was issued "*sua sponte*, without any notice to, or opportunity to be heard by, the parties, the press, or the public." *Id.* The court found that this "blanket order" constituted a "total restraint on the public's first amendment right of access . . ." even though some documents were unsealed after 48 hours. *Id.* at 1147.

In contrast, simply requiring CNS to visit the Prince William courthouse to access any nonconfidential court record it might want does not begin to approach the "total restraint" contemplated by *Associated Press*. And even if it did, not only is precedent from the Ninth Circuit nonbinding, the Ninth Circuit neither applied strict scrutiny nor articulated that strict scrutiny was required under the circumstances presented in *Associated Press*. Accordingly, *Associated Press* is totally inapposite to the case at bar.

Should this Court find that Smith has restricted CNS's access rights, that restriction should be examined under relaxed scrutiny because it resembles a time, place, and manner restriction. Mem. Op. at 10, Dkt. No. 48 (citing *Schaefer*, 2 F.4th at 328; *Glove Newspaper v. Superior Ct.* 457 U.S. 596, 607 n.17 (1982)). "The non-attorney access restriction challenged here does not stop CNS from accessing civil court records altogether but instead controls how and when it accesses them." Dkt. No. 48 at 10. Indeed, CNS can access court records under

Smith's custody by using a public-access terminal at the courthouse during regular business hours. Dkt. No. 55 ¶¶ 25-26. Because the record is devoid of any fact or allegation showing Smith has denied or delayed CNS access to any court record, relaxed scrutiny applies.

**II. The Code of Virginia limits OCRA access to attorneys.**

In an attempt to circumvent the constitutional argument, CNS argues that the Code of Virginia permits Virginia Clerks to grant non-attorneys access to OCRA, because Code §17.1-225 overrides Code § 17.1-293. Dkt. No. 71 at 21 ("Defendants contend that this carve-out [Code § 17.1-293] requires the Clerk to restrict remote access via OCRA to attorneys . . ."); Dkt. No. 71 at 22 ("Section 17.1-225 . . . is [not] limited to systems other than OCRA.") Applying ordinary principles of statutory interpretation, however, shows that the Code is not internally contradictory, and even if it were, the specific language of Code § 17.1-293 trumps the general language of Code § 17.1-225.

"[W]hen [a] statute's language is plain, the sole function of the courts — at least where the disposition required by the text is not absurd—is to enforce it according to its terms." *Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A.*, 530 U.S. 1, 6 (2000). Applying the plain language of competing statutes, statutes employing specific language supersede statutes of general applicability. *Fourco Glass Co. v. Trasmirra Products Corp.*, 353 U.S. 222, 228 (1957). "However inclusive may be the general language of a statute, it will not be held to apply to a matter specifically dealt with in another part of the same enactment." *Id.* (citations omitted). The same principle is used to resolve apparent conflict between two statutes. *See, e.g., United States v. Estate of Romani*, 523 U.S. 517, 532 (1998) (later, more specific statute governs).

CNS argues that Code § 17.1-225 overrides the specific provisions of Code § 17.1-293, because § 17.1-225 generally permits a clerk to provide remote access to records in her custody.

Dkt. No. 71 at 22 ("Section 17.1-225 does not limit remote access to Virginia-barred attorneys, nor is it limited to systems other than OCRA.") Code § 17.1-225 authorizes Virginia clerks to "provide remote access . . . to all nonconfidential court records on an automated case management or other system maintained by his office . . ." *Id.* This section applies to any system the Clerk might use to grant remote access, whether it be OCRA or its own system, such as the Alexandria Justice Information System. *See, e.g.*, Dkt. No. 71-4; *see generally* AJIS2 System, City of Alexandria, https://ajis.alexandriava.gov/default.aspx (last visited July 18, 2022). But Code § 17.1-293 prevents a clerk from disclosing a variety of PII in any context, Va. Code § 17.1-293(A), and from posting certain PII online. Va. Code § 17.1-293(B).[3] In turn, Code § 17.1-293(E)(7) states that the prohibitions in (A) and (B) shall not apply to "[p]roviding secure remote access to nonconfidential court records . . . to members in good standing with the Virginia State Bar and their authorized agents . . ." *Id.* Thus, access to OCRA, described in Code § 17.1-293(E)(7), is clearly limited to attorneys, their staff, and authorized governmental agencies because of its categorical exemption from the dissemination prohibitions articulated in subsections (A) and (B).

Likewise, a plain language interpretation of these two statutes shows no conflict, as Code § 17.1-293, a specific statute, qualifies § 17.1-225, a statute of general applicability. Code § 17.1-225 permits a clerk to provide a system of remote access to court records in her custody; but, under § 17.1-293, if the clerk chooses her own system of remote access, then she must ensure that the information described in Code § 17.1-293(A)-(B) is not posted on that system. If, however, she selects OCRA as her system of remote access, she may forgo the prohibition described in Va. Code § 17.1-293(B) because subsection (E)(7) states that "[t]his section shall

[3] *See also* Dkt. No. 67 at 14 (discussing the types of information prohibited from disclosure in Virginia Code § 17.1-293).

not apply" to providing attorneys and their staff access to nonconfidential court records. *Id.* This plain language interpretation is bolstered by the fact the Virginia General Assembly codified Code § 17.1-225 in 1998. H 1114, 150th Gen. Assemb. Ch. 872 (1998). Eight years later, Virginia codified § 17.1-293, (S 824, H 2062, 154th Gen. Assemb. Ch. 548 (2007), and added (E)(7) four years after that. S 1369, 156th Gen. Assemb. Ch. 715 (2011). Thus, to the extent that the Court sees any conflict between the two statutes, Code § 17.1-293 governs as the later, more specific statute. *Estate of Romani*, 523 U.S. at 532. Accordingly, under Code § 17.1-225, a clerk is permitted to provide remote access to records in her custody although the records must be redacted pursuant to Virginia Code § 17.1-293(B). Pursuant to that authority, if she chooses to provide OCRA as her system of remote access to court records in her custody, then that OCRA access is limited to the individuals described in Code § 17.1-293(E)(7).

## III. OCRA's non-attorney access and dissemination restrictions further the Commonwealth's significant government interest in the fair and orderly administration of justice.

In its Motion for Summary Judgment, the Commonwealth addressed the points raised in CNS's argument that OCRA's non-attorney access and dissemination restrictions are not narrowly tailored to achieving a significant government interest. Dkt. No 71 at 22-28. Specifically, the Commonwealth has addressed the rate at which sensitive information is included in nonconfidential court filings, Dkt. No. 67 at 21-23, and the limited efficacy of redaction and subscriber agreements in preserving privacy, Dkt. No. 67 at 22-24. CNS likewise fails to acknowledge the difference in privacy interests implicated by unlimited remote access versus courthouse visitation. Dkt. No. 67 at 4-5; *supra* at 6-9. Accordingly, CNS fails to show how the Commonwealth's interests would be achieved more effectively utilizing redaction, sealing, and subscriber agreements.

A. CNS completely fails to address the unique privacy concerns raised by remote access to mass quantities of court data.

CNS fails to appreciate how modern technology has sharpened individuals' privacy interest in information compiled by the government. While OCRA contains the same records that are available at the courthouse, Dkt. No. 55 ¶ 49, the facility of complete and instantaneous access to all records within a given jurisdiction via OCRA heightens the potential for abuse of the information contained within those records. CNS ignores this potential for abuse, arguing that because the information is already public, the Commonwealth cannot require the public to visit the court for copies of court records. Dkt. No. 71 at 24. "Defendants only assert[] a general concern about protecting private information without any specifics, and any information that the Clerk seeks to protect is *already public*." *Id.* (emphasis in the original). The Supreme Court has repeatedly rejected CNS's idea that there is no privacy interest in public records. *U.S. Dep't of Def. v. Fed. Labor Relations Auth.*, 510 U.S. at 500 ("An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."). In fact, the government's compilation of personal information into a single place heightens that privacy interest, specifically because it increases the risks of abuse of that information. *Reporters Comm.*, 489 U.S. at 780; *see also Whalen v. Roe*, 429 U.S. 589, 607 (1977) (Brennan, J., concurring). CNS wholly fails to address the unique privacy concerns posed by mass data accessibility, which simply are not implicated by courthouse visitation.

The risk that court records will be abused to the detriment of Virginia litigants is not an abstract threat—Virginia court records *will* be abused by data miners if OCRA is opened to the public. Congress has specifically noted that court records on PACER are regularly mined for data. *See* Data Broker Report at 15. The Data Broker Report went to great lengths to describe

how the digital availability of records on PACER enables data brokers to exploit vulnerable groups. *Id.* at 24, Table 1.

For example, consumer credit reporting company Experian markets a "ChoiceScore" service, which the company asserts "helps marketers identify and more effectively market to under-banked consumers." *Id.* at 25. (citation omitted). "These consumers include 'new legal immigrants, recent graduates, widows, those with a generation bias against the use of credit, followers of religions that historically have discouraged credit,' and 'consumers with transitory lifestyles, such as military personnel.'" *Id.* (citation omitted). Experian suggests using the product to identify these groups, and then target them with direct-marketing offers for risky fiscal transactions such as payday loans, check-cashing services, target invitation-to-apply credit card offers, among others. *Id.* at 26.

The Office of the Attorney General for the State of Vermont has identified even more disturbing lists sold by data brokers and harvested from public records accessed digitally. Office of the Attorney General Department of Financial Regulation, Report to the Vermont General Assembly of the Data Broker Working Group (December 15, 2017), https://ago.vermont.gov/wp-content/uploads/2018/02/2017-12-15-Data-Broker-Working-Group-Report.pdf ("Vermont report"). The Vermont reports references the testimony of Pam Dixon, Executive Director, World Privacy Forum, before the Senate Committee on Commerce, Science, and Transportation on December 18, 2013. *Id.* at 4. She reported that the following list products are available for sale and have been sold by data brokers:

- Rape survivors
- Addresses of domestic violence shelters (which keep their locations secret under law)
- Police officers' and state troopers' home addresses
- Genetic disease sufferers
- Senior citizens suffering from dementia

- HIV/AIDS sufferers
- People with addictive behaviors and alcohol, gambling and drug additions
- People with diseases and prescriptions taken (including cancer and mental illness)
- Consumers who might want payday loans, including targeted minority groups
- People with low consumer credit scores

*Id.* at 8. In addition to making it easier to prey on the financially vulnerable, the Vermont report noted that data brokers enabled stalking and harassing, as well as identity theft, scams, and other forms of fraud. *Id.*; *see also* Data Broker Report at 26 (highlighting how telemarketing criminals purchased name and contact information from a data broker to raid the bank account of a 92-year old Army veteran).

At the state level, there is no real way to prevent or police data brokers' misuse of remotely accessible public records. While some data brokers assert that internal policies "ensure that information is used properly," because data brokers operate in the shadows, with little oversight or regulation "companies in this industry have discretion regarding their voluntary enforcement of such restrictions." *Id.* "Indeed, an investigation into [data broker] InfoUSA showed that employees routinely ignored rules about selling data to known fraudsters," and "three of the largest companies – Acxiom, Experian, and Epsilon – to date have declined to disclose their customers to this Committee." *Id.* (citation omitted).

Mass data harvesting from court records accessed online not only poses a threat to vulnerable individuals, it can pose further threats to national security and democracy. Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, Duke Sanford School of Public Policy, Cyber Policy Program, https://sites.sanford.duke.edu/techpolicy/report-data-brokers-and-sensitive-data-on-u-s-individuals/ (last visited July 21, 2022). For example, data brokers have sold products which can micro-target individuals with election disinformation intended to sow chaos or dissuade voter

participation. *Id.* at 11 (citations omitted). Likewise, data brokers openly and explicitly advertise data on current and former U.S. military personnel, which, because of any lack of accountability, can be sold to organizations which might use the information for "coercion, blackmail, or intelligence-gathering." *Id.* Virginia disproportionately bears this security risk, as the Commonwealth is home to more active duty servicemembers than any other state besides California.[4]

In sum, remote access to mass data poses a bevy of risks to both individuals and society with little accountability for those who abuse access to those records. On the other hand, requiring the public to visit the courthouse to print records minimizes those risks because it shifts the costs of policing abuse to the would-be data harvester. As CNS admits "[i]t is simply not possible for a news service . . . to send reporters on a daily basis, if at all, to the 120 courts throughout the Virginia circuit court system . . ." Dkt. No. 71 at 1. Data brokers face the same limitations. The record is absent of evidence that mass data brokers like Acxiom physically visit courthouses in Virginia to print volumes of court records to mine for information, because doing so is not cost-effective; yet, the record is replete with examples of both data brokers harvesting court records remotely, as discussed *supra*, and unknown entities scraping publicly accessible court databases in Virginia. Declaration of Joby Knuth, Dkt. No. 67-1.

The foregoing illustrates that the concerns articulated by the Supreme Court in *Reporters Committee*, 489 U.S. at 780, have been fully realized: when the government digitally compiles data into a single location, the privacy interest in that information is heightened because its exposure risks abuses not faced when that same information is only available physically. This

[4] U.S. Dep't of Def., 2019 Demographics: Profile of the Military Community, https://download.militaryonesource.mil/12038/MOS/Reports/2019-demographics-report.pdf (last visited July 26, 2022) at 33.

potential for abuse is the key distinction between records made available via courthouse visitation and those made available remotely to anyone, which are routinely and consistently mined for information to the detriment of litigants. OCRA's non-attorney access and dissemination restrictions mitigate the potential for abuse by limiting remote access to lawyers, a pre-vetted group of individuals who have significant professional and personal reasons to refrain from abusing the privilege of remote access.

B. Not only is redaction ineffective at concealing personally identifiable information, redaction laws would not apply to many types of sensitive information.

CNS argues that, in Virginia, "because the filing party is required to redact much of the information Defendants are concerned about . . . a less restrictive alternative is already in place with respect to this particular information." Dkt. No. 71 at 4. The First Amendment, however, does not prevent the Commonwealth from taking additional measures to prevent the widespread dissemination of its litigants' private information. *Ross v. Early*, 746 F.3d 546, 552-53 (4th Cir. 2014) (holding that under relaxed scrutiny "the regulation need not be the least restrictive or least intrusive means of serving the government's significant interests."). Instead, under relaxed scrutiny, this Court need only consider whether the Commonwealth's interest in preventing the widespread dissemination of private information "would be achieved *less effectively* absent the regulation . . ." *Id.* (emphasis added).

Redaction is an ineffective solution in protecting the privacy of litigants. To illustrate this point, in 2010, Paul Ohm, a leading privacy scholar, found that computer scientists "have demonstrated that they can often 'reidentify' or 'deanonymize' individuals hidden in anonymized data with astonishing ease." Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). In particular, Ohm studied three well-known events: the 2006 AOL data release, the Massachusetts Group Insurance

Commission's release of "de-identified" medical records, and the 2006 Netflix prize data study. *Id.* at 1717-1721. Each of these cases revealed that people can be uniquely identified using small amounts of information, such as zip code, birth date, and sex (none of which are protected as "personally identifiable information," or PII, under Virginia law). *Id.* at 1705 (finding that, for 87% of the American population, zero other people share the same combination of ZIP code, birth date, and sex). In response, some areas of federal law, such as HIPAA, have broadened their definitions of redactable PII to include ZIP codes, sex, and birth date. 45 C.F.R. §§ 164.502(d)(2), 164.514(a)-(b) (2000). But privacy scholars have noted that indefinitely broadening what constitutes PII will prove ineffective, because "[w]hile some data elements may be uniquely identifying on their own, *any* element can be identifying in combination with others." Arvind Narayanan & Vitaly Shmatikov, De-Anonymizing Social Networks, https://www.cs.utexas.edu/~shmat/shmat_oak09.pdf (last visited July 26, 2022) at 18 (emphasis in the original).

The Netflix prize data study is particularly revealing as to the inefficacy of redaction because it shows that anonymized individuals can be "reidentified" using trivial personal information, such as how they rate movies. In 2006, in an effort to improve its film recommendations, Netflix publicly released "one hundred million records revealing how nearly a half-million of its users had rated movies from December 1999 to December 2005." Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1720 (2010) (citation omitted). "In each record, Netflix disclosed the movie rated, the rating assigned . . . and the date of the rating," but first "anonymized the records, removing identifying information like usernames, but assigning a unique user identifier to preserve rating-to-rating continuity." *Id.* Only two weeks after the data release, researchers from the University

of Texas announced that people within the database could be easily reidentified and discover all of the movies they have rated with only a little outside knowledge about their movie-watching preferences. *Id.* The resulting report, released in 2008, showed that if an "adversary" knows how a Netflix user had rated six movies, and nothing else, that person could be identified 84 percent of the time. *Id.* (citation omitted). If an adversary knows only two movies a rating user had viewed, with the dates the ratings were made (give or take three days), the adversary can reidentify 68 percent of the users. *Id.* (citation omitted).

Redaction is likewise ineffective at maintaining privacy in court records, as Judge Posner noted in *Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923, 929 (7th Cir. 2004). In that case, quashing a government subpoena for redacted medical records relating to late-term abortions performed at a hospital, Judge Posner stated:

> Some of these women will be afraid that when their redacted records are made a part of the trial record in New York, persons of their acquaintance, or skillful "Googlers," sifting the information contained in the medical records concerning each patient's medical and sex history, will put two and two together, "out" the 45 women, and thereby expose them to threats, humiliation, and obloquy. As the court pointed out in *Parkson v. Central DuPage Hospital* . . . "whether the patients' identities would remain confidential by the exclusion of their names and identifying numbers is questionable at best. The patients' admit and discharge summaries arguably contain histories of the patients' prior and present medical conditions, information that in the cumulative can make the possibility of recognition very high."

*Id.* (quoting *Parkson v. Central DuPage Hospital*, 436 N.E.2d 140, 144 (Ill. 1982)).

Not only is redaction inefficient at concealing the identity of individuals, the redaction requirements in Virginia Code § 8.01-420.8 do not apply to many types of private information harvested by data brokers for exploitation. Code § 8.01-420.8 requires only that a party redact "a social security number or other identification number appearing on a driver's license . . ., or on a credit card, debit card, bank account, or other electronic billing and payment system . . ." *Id.* But

court records contain wide varieties of private information beyond just these listed categories. *See, e.g., David S. Ardia & Anne Klinefelter, Privacy and Court Records: An Empirical Study*, 30 Berkeley Tech. L.J. 1807, 1860 Table 4 (finding that personal information relating to criminal proceedings, identity, and location was present in over half of studied filings in the North Carolina Supreme Court, while personal information relating to health, assets, and financial information was present in 41%, 35%, and 27%, respectively).

There is no reason to believe that records from Virginia would differ from those studied in North Carolina. The Virginia circuit courts process a very high volume of cases with filings reflecting high amounts of sensitive information, such as domestic relations cases (11, 921 cases in 2021), felonies (103,920 in 2021), and probate matters (3,005 in 2021). Caseload Statistical Information: Circuit Court Caseload reports, Virginia's Judicial System, cr01_2021_dec.pdf (vacourts.gov) (last visited July 27, 2022); *see also id.* at cr01_2021_dec.pdf (vacourts.gov) (reflecting filings by case category in the Circuit Court of Prince William County). If made available online, redaction would not protect any of the sensitive information contained in these filings, which would be harvested and sold by data brokers to the detriment of, for example, rape victims, genetic disease sufferers, and senior citizens, to name only a few. *See* discussion of data broker lists, *supra* at 13-14.

C. Sealing court records is inefficient and ineffective at protecting private information.

CNS argues that a "less restrictive alternative is already in place with respect to minor and maiden names" in the form of sealing. Dkt. No. 71 at 25. But for the same reasons redaction is ineffective at preventing mass data harvesting, so is sealing. The two examples of sealing offered by CNS simply do not address the private information described in the 2015 Empirical Study. Nor would more sealing address Virginia's interest in the fair and orderly administration

of justice. Sealing is a burdensome and expensive process for the court and litigants and expanding Virginia's sealing requirements would prompt more First Amendment litigation, as many of the cases to which CNS cites make plain. *See, e.g., Va. Dept. of State Police v. Washington Post*, 386 F.3d 567 (4th Cir. 2004); *Associated Pres v. Dist. Ct.*, 705 F.2d 1143 (9th Cir. 1983); *Doe v. Public Citizen*, 749 F.3d 246 (4th Cir. 2014).

D. Subscriber agreements have proven ineffective at preventing data harvesting.

Finally, CNS suggests that private information available on OCRA will not be subject to widespread dissemination if opened to the public because subscriber agreements ensure that "OCRA records are not available to any anonymous internet user." Dkt. No. 71 at 26. But PACER, which likewise requires a subscription fee and user agreement, is mined by data brokers routinely. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 457 (2008). Nor have PACER's subscriber requirements proven effective at preventing significant data breaches. Maggie Miller, Justice Department Investigating Data Breach of Federal Court System (July 28, 2022, 8:49PM), https://www.politico.com/news/2022/07/28/justice-department-data-breach-federal-court-system-00048485 (discussing House Judiciary Committee Chair Jerrold Nadler's report that "three hostile foreign actors" had attacked the federal judiciary's Case Management/Electronic Case Files system); United States Courts, Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records (January 6, 2021), https://www.uscourts.gov/news/2021/01/06/judiciary-addresses-cybersecurity-breach-extra-safeguards-protect-sensitive-court. Likewise, OES has confirmed that at least one subscriber-based database it maintains is regularly scraped for social security numbers. *See* Dkt. No. 67 at 23-24 (discussing current data-scraping of the OES-maintained Virginia Date of Birth

Confirmation system).

CNS argues that these "less restrictive safeguards work" in preventing widespread dissemination of private information but fails to provide any empirical data in support of that assertion. Dkt. No. 71 at 26. Under relaxed scrutiny, the Court need only consider how *effective* these alternative restrictions would be at protecting sensitive information from widespread disclosure, because a "regulation will not be invalid simply because a court concludes that the government's interests could be adequately served by some less-speech restrictive alternative." *Ward v. Rock Against Racism*, 491 U.S. 781, 800 (1989). In this case, the overwhelming weight of empirical evidence shows that the Commonwealth's interest in protecting the privacy of its litigants would be achieved far less effectively if it made court records generally available via remote public access.

## IV. CNS has failed to show it is entitled to injunctive relief.

### A. CNS has failed to show that it will suffer irreparable injury.

CNS has failed to show it will suffer irreparable injury absent an injunction because it can immediately access court records in the Prince William Circuit Court. CNS argues that "access restrictions that violate the First Amendment necessarily constitute irreparable harm," citing *Legend Night Club v. Miller*, 637 F.3d 291 (4th Cir. 2011). But in *Legend*, the appellants challenged a statute which would revoke their license to sell alcoholic beverages if the night club allowed certain attire and conduct on business premises. *Id.* at 295-96. In that case, the "threatened injury" was the imminent threat of license revocation, which would significantly affect the night club's business operations. *Id.* at 302. "At a minimum, each Plaintiff faces a loss of its license coupled with a loss of valuable business opportunities." *Id.*

In contrast, CNS has not articulated a future injury that CNS will incur should the Court

deny its request for an injunction. CNS will continue to visit the Prince William Courthouse each day to collect civil filings, where it can view every civil filing it desires "immediately," as CNS has stipulated. Dkt. No. 71 ¶ 35. This "restriction" of having to visit the courthouse to obtain copies of court filings has never been found to violate the First Amendment, nor would it affect CNS's current business practices.

B. The balance of equities and the public interest favor the Commonwealth.

CNS argues that there "can be no irreparable harm to a governmental entity when it is prevented from enforcing an unconstitutional statute . . ." Dkt. No. 71 at 30 (citation and internal quotations omitted). CNS has neither identified any harm it will incur in the future should the Court refrain from issuing an injunction, nor articulated why having to visit the courthouse to view court records is unconstitutional. On the other hand, the Commonwealth and Smith will both suffer substantial hardships should the Court require OCRA be opened to the public. *See* Declaration of Michael Riggs, Dkt. No. 67-1 at 9, ¶ 6 (discussing the cost of OCRA to Virginia clerks). If an injunction is granted, if a clerk chooses to continue offering OCRA, pursuant to Code § 17.1-293(B), the clerk would be forced to redact every single record in her custody before posting to OCRA, both civil and criminal. As Smith has identified, this would significantly increase redaction costs. Declaration of Paul Ferguson, Dkt. No. 67-3 at 2, ¶ 11. Should a clerk decide that redaction would be too costly, the Clerk may forgo offering OCRA altogether, resulting in wasted costs in purchasing and maintaining electronic servers stored at the courthouse. Dkt. No. 67-1 at 1-2, ¶ 3. Such a decision would carry a high cost to Virginia litigants as well, as their lawyers would instantaneously lose remote access to court records, frustrating the administration of justice. Time spent traveling to and from courthouses, and funds spent on printing pages, would be passed from lawyers on to the litigants. And finally, Virginia

litigants would suffer immeasurable costs in terms of privacy exposure to data brokers, scam artists, and stalkers, as discussed *supra*.

## CONCLUSION

Wherefore, for the foregoing reasons, the Commonwealth respectfully requests that this Court deny Courthouse News Service's Motion for Summary Judgment, and award the defendants any further relief that the Court deems necessary and proper.

Respectfully submitted,

COMMONWEALTH OF VIRGINIA

By: */s/ Robert B. McEntee, III*
Counsel

Jason S. Miyares
*Attorney General*

Steven G. Popps
*Deputy Attorney General*

Jacqueline C. Hedblom
*Senior Assistant Attorney General/*
*Acting Trial Section Chief*

Robert B. McEntee, III (VSB No. 89390)
Erin R. McNeill (VSB No. 78816)
Assistant Attorneys General
Office of the Attorney General
202 North Ninth Street
Richmond, Virginia 23219
(804) 786-8198 – Telephone
(804) 371-2087 – Facsimile
rmcenteeiii@oag.state.va.us
emcneill@oag.state.va.us

## CERTIFICATE OF SERVICE

I hereby certify that on August 1, 2022, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to all counsel of record for the parties.

*/s/ Robert B. McEntee, III*
Robert B. McEntee, III